Lowenstein Sandler's Cybersecurity Awareness Series

Session 12 – The Impact of the 2024 CrowdStrike Incident on Cyber Insurance

By Lynda A. Bennett and Ken Fishkin

OCTOBER 2024

Ken Fishkin: Hello, and welcome to another episode of **Lowenstein Sandler's Cybersecurity Awareness series**. I'm here with Lynda Bennett, partner and Chair of the **Insurance Recovery Group**, and today we'll be discussing the recent CrowdStrike incident and its impact on the cyber insurance industry.

In a nutshell, the CrowdStrike incident caused roughly 8.5 million systems to crash, impacting airports, health care facilities, government services, and many other industries. And it was all due to improper quality assurance testing of a configuration update.

So, Lynda, now that all these companies are scrambling trying to come up with incident response plans to make sure that this doesn't happen again to them, what are insurance carriers doing?

Lynda A. Bennett: Well, thanks for **having me back**, Ken; you know I always love geeking out about insurance.

So, the cyber market continues to be what I like to characterize as "a little bit of the Wild West." There is tremendous variation in policy terms and conditions across different insurance companies, and the way that the market is specifically responding to these types of events is in a wide variety of ways. So, we're starting to see some narrowing of coverage through the use of sublimits, waiting periods, and--particularly for these larger scale events—some insurers are starting to put endorsements on their policies that restrict coverage when there is this type of wide-scale event.

Ken Fishkin: So, since the incident was not cyber-related, would it be covered under your cyber insurance policy?

Lynda A. Bennett: CrowdStrike was interesting because it was negligence-based, and the insurance industry is looking at a spectrum of risk that they're willing to insure. And from my point of view, CrowdStrike is closer to the kind of risk that the industry does not want to insure under cyber policies. They're really interested in having this product be more geared toward the threat actor, malicious act, ransomware type of event. That being said, for

CrowdStrike—as with every insurance dispute that I deal with—the devil is really in the detail of the insurance policies themselves.

Many companies, however, at least in the United States, likely didn't have a covered claim because a lot of these cyber policies include waiting periods. So, as you know, CrowdStrike really originated over in East Asia, and by the time the people in the United States woke up, the patch was already out there, and so, under a cyber policy that has an 8-to-12-hour waiting period of having to be down before coverage can be triggered, in the CrowdStrike incident many companies likely didn't have a viable claim to pursue.

Ken Fishkin: I know that there are many new security measures that are now required by insurance carriers—such as multi-factor authentication, security awareness training—but do you see any new measures that are coming down the pike?

Lynda A. Bennett: I think the biggest thing that we've learned from the most recent widespread event type of incident is the interdependence of supply chain. So, really looking at not only your own risk profile, but all of the entities and businesses that you're doing business with or that you rely on to provide access to your information is something that the insurance industry is going to be asking you about when you're going through the underwriting process. But there's another way to start managing that risk, which is through your own contracts with those vendors. So, you can look at imposing insurance requirements on them, also imposing contractual indemnification on them.

So, I think the biggest learning lesson that's coming out of CrowdStrike and these widespread events like that is the interdependence that we have as everyone's moving information to the cloud—how secure is that? And what are those other risk management tools that you can use besides insurance to protect yourself? So that would be, you know, looking very carefully at your contractual relationships with your vendors. You know, as I said, you can get a contractual indemnification from those vendors, but you also have to think about whether that will be nice words on a page or whether they'll also have the financial wherewithal to back that up when you get that type of protection in place.

Ken Fishkin: When reviewing your policy, what are some key sections that you need to watch out for so you can avoid some potential gotchas?

Lynda A. Bennett: Unfortunately, Ken, you have to read the whole policy, and that's something that a lot of people don't like to do. Fortunately, me and the Insurance Recovery Group here at Lowenstein Sandler do like to read policies, and I really want to impress upon your viewers the importance of doing that, because these terms and conditions are negotiable. At the front end, you need a quality broker. You need experienced coverage counsel to review these and negotiate these before a claim ever comes in. And we're looking very carefully at the definitions, the exclusions. And as I mentioned, these sublimits or other endorsements that are taking

what looks like a $25 million policy when you look at the front page, by the time you get to page 93 of this policy, you'll find out that for certain types of events, you may only have coverage for $5 million. So, it really is, you've got to dive into the details of the words, negotiate those terms and conditions before the policy is bound, and then obviously carefully review in the event of a claim to know what's what.

Ken Fishkin: Well, thank you for joining me today, Lynda. And thank you to our viewers for joining us, and we'll see you next time.